MMT and CMR Launchpad Integration

Summary

Spec Workshop Date: 4/10/2017

Attendees:

Background Information:

This specification workshop is to help us understand the goal of Launchpad integration and identify what all EOSDIS components would be impacted by the integration.

Goal of this feature: Ensure only providers with valid auid credentials are able to modify CMR metadata and business objects (e.g. groups, permissions, service options) while still ensuring that search and order permissions are available based on Earthdata Login profile.

Key User Stories

As a provider, I want to login to MMT with my auid.

As a provider, I want to set collection permissions based on Earthdata Login ID.

As a provider, I want to set provider permissions based on auid.

As an operations team, I want to set system object permissions based on auid.

As a non-EOSDIS provider, I want to submit a collection to a holding place where a auid verified reviewer can approve the collection for submittal to the CMR. — optional, would help replace docBuilder

MMT

- Integrate with auid
- Rework workflow so it is clear to users which ID/profile to use
-

Known Deadlines

None, but we need to be continually making progress.

Rough Sizing Estimates

Notes

Initial email notes:

Option A:

1) User logs into MMT with **auid**.

2) MMT **converts the auid to a Earthdata Login id** and sends the user’s Earthdata Login name to the CMR.

3) The CMR looks up what permissions that user has based on **Earthdata Login id**. (e.g. “User can create data for provider Y”, “User is a system user who can modify everyone else’s permissions”, “User can delete orders for provider Y”, etc.)

4) The MMT then limits the user’s functionality to only what they have permissions to do.

Option B:

1) User logs into MMT with **auid**.

2) MMT sends the user's **auid** to the CMR.

3) The CMR looks up what permissions that user has based on **auid**. (e.g. "User can create data for provider Y", "User is a system user who can modify everyone else's permissions", "User can delete orders for provider Y", etc.)

4) The MMT then limits the user's functionality to only what they have permissions to do.

A few notes:

- Today, clients other than MMT allow for editing of metadata. They are all based on Earthdata Login ID since CMR's permissions model are based on Earthdata Login. MMT is only 1 client. (Note: some systems use a "system id" which is a little different than an Earthdata Login ID)
- Option B would require a fairly substantial rewrite to CMR's permission service. Currently, one permission model controls both ingest and search permissions and it is all based on earthdata login. We ***could*** separate and make ingest permissions controlled via auid and search permissions controlled via earthdata login to at least minimize impacts to clients and end users.

Questions:

- How should system groups be treated in this model? – shouldn't be impacted
- What is the expected behavior of automated providers (SDPS, etc.)? – NAMS has the concept of a system user, need to explore password expiration options
- What is the expected behavior for international providers? – holding place until auid user review/approval/submittal

----

*CMR needs to ensure that NAMS token being passed in is valid (delegated authentication)

* Providers all need tokens (should be ok)

- Need to migrate existing permissions
- Wait on Crowd analysis (could it be the common solution)